99187406 EP

CERTIFICATE

I, the undersigned, Toshio KAWAHARA, residing at 1-34-5, Asagaya-kita, Suginami-ku, Tokyo, JAPAN, hereby certify that to the best of my knowledge and belief the following is a true translation into English made by me of Japanese Patent Application No. P10-360720 filed on December 18, 1998.

Dated this 22nd day of November, 1999

Toshio Kawahara

Toshio KAWAHARA

[Name of Document] Application for Patent

[Reference No.] A009806612

[Application Date] December 18, 1998

[Destination] Commissioner, Patent Office

[International Patent Classification] G03G 15/00

[Title of the Invention] Ticket issue method and ticket check method

[No. of Claims] 13

[Inventor]

[Address] 70, Yanagi-cho, Saiwai-ku, Kawasaki-shi, Kanagawa-ken
Toshiba Yanagi-cho Works

[Name] Takashi Yamaguchi

[Applicant for Patent]

[Identification No.] 000003078

[Name] Toshiba Corporation

[Agent]

[Identification No.] 100058479

[Patent Attorney]

[Name] Takehiko Suzue

[Telephone No.] 03-3502-3181

[Assigned Agent]

[Identification No.] 100084618

[Patent Attorney]

[Name] Sadao Muramatsu

[Assigned Agent]

[Identification No.] 100068814

[Patent Attorney]

[Name] Jun Tsuboi

[Assigned Agent]

[Identification No.] 100092196

[Patent Attorney]

[Name] Yoshio Hashimoto

[Assigned Agent]

[Identification No.] 100091351

[Patent Attorney]

[Name] Tetsu Kono

[Assigned Agent]

[Identification No.] 100088683

[Patent Attorney]

[Name] Makoto Nakamura

[Assigned Agent]

[Identification No.] 100070437

[Patent Attorney]

[Name] Shoji Kawai

[Designation of Charge]

[Ledger No. of Prepayment] 011567

[Amount of payment] 21000 yen

[List of Filed Document]

[Object Name] Specification 1

[Object Name] Drawing 1

[Object Name] Abstract 1

[Necessity of Confirmation]   Necessary

[Name of Document] Specification

[Title of the Invention] Ticket Issue Method and Ticket Check Method

[What is Claimed is]

[Claim 1] A ticket issue method characterized in that said method generates security data from ticket issue request data sent from a user via communication means and user identification data, also generates ticket image data from said ticket issue request data, embeds said generated security data in said generated ticket image data in the invisible state, thus generates ticket print data for printing a ticket by said user, and sends said generated ticket print data to said user via communication means.

[Claim 2] A ticket issue method according to Claim 1, wherein said method generates said security data by binarizing basic security data composed of a control code, characters, images, and voice, generating binary embedded data, and then converting the same to binary image data in the predetermined specific format.

[Claim 3] A ticket issue method according to Claim 1, wherein said method generates ticket print data by generating predetermined pattern image data, generates pattern modulated image data by modulating said generated pattern image data according to said security data, and superimposing said generated pattern modulated image data on said ticket image data.

[Claim 4] A ticket issue method according to Claim 3, wherein when generating said predetermined pattern image data, adjacent image data are colored by a combination of complementary colors.

[Claim 5] A ticket issue method according to Claim 1, wherein said method reduces a part of data from said ticket print data, generates ticket display data for confirming display by display means by said user, and sends said generated ticket display data to said user together with said ticket print data via communication means.

[Claim 6] A ticket issue method according to Claim 5, wherein said method generates said ticket display data so as to ascertain that a part of data is reduced from said ticket print data by smoothing said ticket print data and then thinning out said data.

[Claim 7] A ticket issue method according to Claim 1, wherein a part of said security data is embedded in said ticket image data in both invisible state and visible state.

[Claim 8] A ticket issue method according to

Claim 1, wherein a part of said security data is embedded in said ticket image data in both invisible state and visible state and the embedded positions thereof coincide with each other.

[Claim 9] A ticket issue method according to Claim 1, wherein a specific mark for distinguishing from ticket image data having no embedded security data is added to said ticket image data generated by embedding said security data in the invisible state in the visible state.

[Claim 10] A ticket issue method according to Claim 1, wherein said security data comprises user identification data, ticket issue date and time data, ticket kind data, ticket validity term data, ticket charge data, and control data.

[Claim 11] A ticket check method for generating security data from ticket issue request data sent from a user via communication means and user identification data, also generating ticket image data from said ticket issue request data, further generating predetermined pattern image data, generating pattern modulated image data by modulating said generated pattern image data according to said generated security data, generating ticket print data by superimposing said generated pattern modulated image data on said generated ticket image data, sending said generated ticket print data to said user via communication means, and discriminating the truth of tickets issued by said ticket issue method by which said user prints a ticket on the basis of said sent ticket print data, wherein by physically superimposing a sheet-shaped mask having the transmission distribution rate of the same pattern as that of said pattern image data on said issued ticket print surface, said ticket check method makes said security data visible and restores said data and discriminates the truth according to said restored security data.

[Claim 12] A ticket check method for generating security data from ticket issue request data sent from a user via communication means and user identification data, also generating ticket image data from said ticket issue request data, further generating predetermined pattern image data, generating pattern modulated image data by modulating said generated pattern image data according to said generated security data, generating ticket print data by superimposing said generated pattern modulated image data on said generated ticket image data, sending said generated ticket print data to said user via communication means, and discriminating the truth of tickets issued by said ticket issue method by which said user prints a ticket on the basis of said sent ticket print data, wherein said method optically reads the ticket surface data of said issued ticket, compares said obtained read signal with the mask signal representing the same pattern as that of said pattern image data, restores said security data by making the matched portion of the two invalid, and discriminates the truth according to said restored security data.

[Claim 13] A ticket check method for generating security data from ticket issue request data sent from a user via communication means and user identification data, also generating ticket image data from said ticket issue request data, further generating predetermined pattern image data, generating pattern modulated image data by modulating said generated pattern image data according to said generated security data, generating ticket print data by superimposing said generated pattern modulated image data on said generated ticket image data, sending said generated ticket print data to said user via communication means, and discriminating the truth of tickets issued by said ticket issue method by which said user prints a ticket on the basis of said sent ticket print data, wherein said method optically reads the ticket surface data of said issued ticket, restores said security data by performing the thinning-out process for said obtained read signal in the cycle corresponding to the spatial frequency of said pattern image data, and discriminates the truth according to said restored security data.

[Detailed Description of the Invention]

[0001]

[Background of the Invention]

The present invention relates to, for example、a ticket issue method for issuing tickets of a concert or coupons of means of transportation via a network or telephone lines.

[0002]

Further, the present invention relates to a ticket check method for discriminating the truth of tickets and coupons issued by the aforementioned ticket issue method.

[0003]

[Prior Art]

Recently, a system that a ticket of a concert or a coupon of a means of transportation is reserved using a network or telephone line and the applicant goes and receives the reserved ticket at the predetermined location is wide spread and anyone can get a ticket while staying at home or in the company.

[0004]

Furthermore, due to spread of personal computers and color printers and fixing of the infra-structure of the communication environment such as Internet, a system that a ticket reserved via a network can be directly issued at home or in the company has been examined.

[0005]

For example, recently, a service that a ticket of a concert is reserved via a network, and a ticket exchange image is down loaded on the personal computer at home, and the image is stored on a floppy disk, and it is brought to the concert place, and hence the applicant can see the concert is given.

[0006]

A system that an electronic stamp is reserved via a network and the electronic stamp is issued at home or in the company has also been experimented. As an example thereof, in USP5606507 and USP5666284, a method and a stem for storing stamp data including coded postage data in a dedicated storage device connected to a personal computer and then printing it are proposed.

[0007]

[Problems that the Invention is to Solve]

In USP5606507 and USP5666284, a dedicated storage device to be connected to a personal computer is necessary, so that the client system constitution is limited. Although postage data is coded, it is printed on an envelope or others in the visible state using the two-dimensional bar code art or the applied art thereof, so that there is a defect that it can be decoded comparatively easily by taking and comparing two differences and the security is weak.

[0008]

Therefore, an object of the present invention is to provide a ticket issue method which can simply issue tickets with high security via a communication means such as a network or telephone lines.

[0009]

Another object of the present invention is to provide a ticket check method which can simply discriminate the truth of tickets issued by the aforementioned ticket issue method and easily conduct a follow-up study when a false ticket is found.

[0010]

[Means of Solving the Problems]

The ticket issue method of the present invention is characterized in that it generates security data from ticket issue request data sent from a user via a communication means and user identification data, also generates ticket image data from the ticket issue request data, embeds the generated security data in the generated ticket image data in the invisible state, thus generates ticket print data for printing a ticket by the user, and sends the generated ticket print data to the user via a communication means.

[0011]

The ticket issue method of the present invention is characterized in that it generates security data by binarizing the basic security data composed of a control code, characters, images, and voice, generating binary embedded data, and then converting it to binary image data in the predetermined specific format.

[0012]

The ticket issue method of the present invention is characterized in that it generates ticket print data by generating predetermined pattern image data, generates pattern modulated image data by modulating the generated pattern image data according to the security data, and superimposing the generated pattern modulated image data on the ticket image data.

[0013]

The ticket check method of the present invention is a ticket check method for generating security data from ticket issue request data sent from a user via a communication means and user identification data, also generating ticket image data from the ticket issue request data, further generating predetermined pattern image data, generating pattern modulated image data by modulating the generated pattern image data according to the generated security data, generating ticket print data by superimposing the generated pattern modulated image data on the generated ticket image data, sending the generated ticket print data to the user via a communication means, and discriminating the truth of tickets issued by the ticket issue method by which the user prints a ticket on the basis of the sent ticket print data and the ticket check method is characterized in that by physically superimposing a sheet-shaped mask having the transmission distribution rate of the same pattern as that of the aforementioned pattern image data on the issued ticket print surface, the ticket check method makes the security data visible and restores it and discriminates the truth according to the restored security data.

[0014]

The ticket check method of the present invention is a ticket check method for generating security data from ticket issue request data sent from a user via a communication means and user identification data, also generating ticket image data from the ticket issue request data, further generating predetermined pattern image data, generating pattern modulated image data by modulating the generated pattern image data according to the generated security data, generating ticket print data by superimposing the generated pattern modulated image data on the generated ticket image data, sending the generated ticket print data to the user via a communication means, and discriminating the truth of tickets issued by the ticket issue method by which the user prints a ticket on the basis of the sent ticket print data and the ticket check method is characterized in that it optically reads the ticket surface data of the issued ticket, compares the obtained read signal with the mask signal representing the same pattern as that of the pattern image data, restores the security data by making the matched portion of the two invalid, and discriminates the truth according to the restored security data.

[0015]

Furthermore, the ticket check method of the present invention is a ticket check method for generating security data from a ticket issue request sent from a user via a communication means and user identification data, also generating ticket image data from the ticket issue request data, further generating predetermined pattern image data, generating pattern modulated image data by modulating the generated pattern image data according to the generated security data, generating ticket print data by superimposing the generated pattern modulated image data on the generated ticket image data, sending the generated ticket print data to the user via a communication means, and discriminating the truth of tickets issued by the ticket issue method by which the user prints a ticket on the basis of the sent ticket print data and the ticket check method is characterized in that it optically reads the ticket surface data of the issued ticket, restores the security data by performing the thinning-out process for the obtained read signal in the cycle corresponding to the spatial frequency of the pattern image data, and discriminates the truth according to the restored security data.

[0016]

According to the present invention, security data is generated from a ticket issue request sent from a user via a communication means and user identification data, and also ticket image data is generated from the ticket issue request data, and the generated security data is embedded in the generated ticket image data in the invisible state, and hence ticket print data is generated, and the generated ticket print data is sent to the user via a communication means, and the user prints a ticket according to the sent ticket print data, thus the security data can be embedded in the ticket print data in the invisible state, so that tickets with high security can be simply issued via a communication means such as a network or telephone lines.

[0017]

According to the present invention, by physically superimposing a sheet-shaped mask having the transmission distribution rate of the same pattern as that of the pattern image data on the issued ticket print surface by the ticket issue method, the security data is made visible and restored or the ticket surface data of the ticket issued by the ticket issue method is optically read, and the obtained read signal is compared with the mask signal representing the same pattern as that of the pattern image data, and the security data is restored by making the matched portion of the two invalid, or the ticket surface data of the ticket issued by the ticket issue method is optically read, the security data is restored by performing the thinning-out process for the obtained read signal in the cycle corresponding to the spatial frequency of the pattern image data, and the truth is discriminated according to the restored security data and hence the security data of the used ticket can be simply taken out, so that a follow-up study when a false ticket is found can be easily conducted.

[0018]

[Embodiments of the Invention]

The embodiments of the present invention will be explained hereunder with reference to the accompanying drawings.

[0019]

Fig. 1 schematically shows the constitution of a ticket issue system for realizing the ticket issue method relating to the present invention. The ticket issue system is structured by connecting an apparatus A on the user side and an apparatus B on the system side with a network C such as Internet or a LAN.

[0020]

The apparatus A on the user side comprises a user terminal device 11 composed of a personal computer, dedicated client software 12 operating on the personal computer, and a ticket printer 13 such as a color printer to be connected to the user terminal device 11.

[0021]

The apparatus B on the system side comprises a host computer/server 16, dedicated server software

17 operating on the host computer, a data base 18 storing ticket data, user data, and other data, and a security data detecting system 19.

[0022]

Next, the ticket issue method will be explained by referring to the flow chart shown in Fig. 2. It is assumed that the host computer/server 16, the dedicated server software 17, and the data base 18 are always activated and a user registered in the data base 18 is in the state that he can use them at any time.

[0023]

Firstly, the user starts the user terminal device 11 and the dedicated client software 12 (S1), inputs user identification data such as a user ID and a password (S2), and connects them to the host computer/server 16 (S5).

[0024]

The host computer/server 16 checks the sent user identification data with the data in the data base 18 (S3), permits connection when there is user identification data in the registered person list (S4), starts the service, and rejects connection when there is no user identification data in the registered person list.

[0025]

When the connection to the host computer/server 16 starts (S5), the service menu is displayed on the user terminal device 11 and the user selects the desired service and inputs the ticket issue request data (S8). In this case、the ticket issue request data is, for example, in the case of the ticket purchase service, necessary data such as the desired ticket kind, date and time, charge, seat, and charge payment means.

[0026]

When the ticket issue request data is input, the user terminal device 11 sends those input data to the host computer/server 16 and the host computer/server 16 receives them, checks them with the data in the data base 18 (S9), and performs the ticket purchase procedure. When no ticket can be purchased, the host computer/server 16 sends the data to the user terminal device 11 as a message and the service menu is displayed again.

[0027]

When a ticket can be purchased, the host computer/server 16 generates security data from the ticket issue request data and user identification data (S10), also generates ticket image data from the ticket issue request data (S11), and embeds the security data in the ticket image data in the invisible state, and then generates ticket print data (S12). Further, the host computer/server 16 generates ticket display data on the basis of the ticket print data (S13) and sends the ticket print data and ticket display data to the user terminal device 11 (S14). Detailed generation of the security data, ticket print data, and ticket display data will be described later.

[0028]

On the display of the user terminal device 11, the ticket display data sent from the host computer/server 16 is displayed (S15), and the user sees and checks the display, and when there is no problem, he prints a ticket. Namely, when the print instruction is executed, the ticket print data is sent to the ticket printer 13 from the user terminal device 11 and a ticket 14 is printed and output (S16). When the printing terminates normally, the print termination instruction is executed and when a print error occurs, the print instruction is executed again.

[0029]

The user brings the printed ticket 14 to the concert place and can use it as usual (S17). In the concert place, the used ticket 14 is checked for a normal ticket using the security data detecting system 19. The security data detecting system 19 checks the detected security data with the data in the data base 18 and discriminate the truth thereof (S18).

[0030]

Figs. 3 to 5 show examples of concert tickets to be applied to this embodiment. Fig. 3 schematically shows ticket image data 21, Fig. 4 security data 22, and Fig. 5 a ticket print data 23.

[0031]

The ticket image data 21 shown in Fig. 3 is generated from the ticket issue request data by referring to the data base 18 in the process of Step S11 shown in Fig. 2 and on it, a ticket kind 31, a place 32, a date and time 33, a seat 34, a charge 35, a serial No. 36 used for inquiry, a ticket issuer 37, and a logo mark 38 which are necessary for tickets used in an ordinary concert are recorded. These data are also recorded on the stub of a ticket.

[0032]

The security data 22 shown in Fig. 4 is generated from the user identification data and ticket issue request data in the process of Step S10 shown in Fig. 2 and the data is used to discriminate the truth of whether a ticket is forged or falsified or not. In this example, data such as two-dimensional bar code data 39, a serial No. 40 for inquiry, a ticket issuer 41, and a logo mark 42 is recorded. These data including characters and figures are represented as binary images.

[0033]

The two-dimensional bar code data 39 shown in Fig. 4 is recorded so as to perform the automatic process by the machine when the security data 22 is read and in it, the ticket kind 31, the place 32, the date and time 33, the seat 34, the charge 35, the serial No. 36, the ticket issuer 37, and the logo mark 38 recorded in Fig. 3 are converted to two-dimensional codes and recorded. The data of the serial No. 40 for inquiry, the ticket issuer 41, and the logo mark 42 is provided so as to check the security data 22 with the naked eye.

[0034]

The serial Nos. 36 and 40 for inquiry are, for example, 20-digit numbers in this embodiment. In this case, they are composed of the data shown in Table 1 below.

[0035]

[Table 1]

Classification	No. of Figure	Data Example	Use
Serial No.	20	1998092512345678	Used for inquiry to Data Base
Date of Issue	8	19980926	Date
Class. Code 1	2	12	Data Base Class. Code
Class. Code 2	4	3412	Kind of Ticket/Area/ Form of Contract, etc.
Ticket No.	6	345678	Ticket Issue Order

[0036]

In Table 1 shown above, the issue date indicates the date when a ticket is reserved, the classification code 1 the data storage position of the data base for retrieval, the classification code 2 the ticket kind and others which are coded, and the ticket No. the issue order. Using the serial number composed of these data as a checking key for the data base 18, a large quantity of tickets can be controlled integratedly.

[0037]

As mentioned above, the security data 22 shown in Fig. 4 can be checked by both a machine and a person. These data are also recorded on the stub of a ticket.

[0038]

The ticket print data 23 shown in Fig. 5 is generated from the security data and ticket image data in the process of Step S12 shown in Fig. 2 and when the data is printed, an actual ticket is obtained.

The ticket print data 23 shown in Fig. 5 is generated by embedding the security data 22 shown in Fig. 4 in the ticket image data 21 shown in Fig. 3 in the invisible state by the method which will be described later, so that Figs. 3 and 5 are exactly the same when seen with the naked eye and can be little distinguished from each other.

[0039]

In this embodiment, the serial number for inquiry, ticket issuer, and logo mark of the ticket issuer are added to the ticket image data in the visible state and to the security data in the invisible state. By adding partial data of a ticket in the visible state and in the invisible state like this, forging and falsifying of a ticket by simple rewriting can be detected immediately.

[0040]

With respect to the logo marks, they are arranged so that the positions thereof in the visible state and the invisible state perfectly coincide with each other. By doing this, it is very difficult to forge or falsify either one or both of the logo marks in the visible state and the invisible state and the security of tickets increases furthermore.

[0041]

Next, how to generate security data will be explained.

[0042]

The security data, as shown in Fig. 4, comprises two-dimensional bar code data and a binary image and it may comprise either one of the elements or both of the elements.

[0043]

When a two-dimensional bar code is used, the mechanical process is available to detect the security data and when a binary image is used, the process by the human sense of sight is available and they can be changed according to the system characteristics. Each of the two-dimensional bar code and binary image constituting the security data is called basic security data.

[0044]

An example of generation of the two-dimensional bar code 39 shown in Fig. 4 will be explained hereunder.

[0045]

The two-dimensional bar code 39 is, as described above, recorded to perform the automatic process by the machine when the security data is read and in it, the ticket kind and others are coded and recorded. In this case, data to be two-dimensionally coded includes almost every kind of type such as not only the ticket kind but also individual data such as the voiceprint and fingerprint of a user already registered, control data, voice, image, and text.

[0046]

Firstly, it is necessary to convert the basic security data to digital data. When the basic security data is composed of analog data such as voice and voiceprint, it is subjected to A-D conversion and converted to digital data. When the basic security data is data in the digital data format, it is used as it is.

[0047]

Next, the digitized basic security data is converted to a binary image by the two-dimensional code. For that purpose, the basic security data is divided into 4-bit blocks sequentially from the beginning and each block is replaced with black-and-white binary image data of 2x2 pixels as shown in Fig. 6 according to each block value.

[0048]

For example, assuming that the embedded data is lined up in hexadecimal representation from the beginning as shown below:

FF 01 45 D3 ---,

these are replaced as shown in Fig. 7.

[0049]

Furthermore, the binary image data (Fig. 6) is extended to n times so as to prevent the embedded image data from damage during the smoothing process at the time of the synthetic process which will be described later. In this case, it is desirable that n = 2 to 4. For example, assuming that n = 2, the result when the binary image data shown in Fig. 7 is extended is shown in Fig. 8.

[0050]

In this embodiment, the Calra code is applied to two-dimensional coding. However, two-dimensional codes of other matrix systems or two-dimensional bar codes such as the Glyph code may be used without trouble.

[0051]

When a character string 41 of "Ticket east, west, south, north" as shown in Fig. 4 and binary image data of the logo mark 42 are to be added to the security data, these data are converted to binary image data. In this case, it is necessary to unify the image resolution for conversion and it is desirable to make it coincide with the image resolution of the ticket print data. The significant portion such as characters is converted to a black component and the meaningless portion such as the background is converted to a white component.

[0052]

The two-dimensional bar code data and binary image data generated in this way are laid out in the area of the same size as that of the ticket image data as shown in Fig. 4. It is necessary to decide the layout position beforehand according to the system for reason of the sensor when detecting the security data.

[0053]

Next, the ticket print data generation method (synthetic process method) will be explained in detail by referring to Fig. 9.

[0054]

Ticket image data 21 is so-called data of ticket itself and equivalent to Fig. 3. It has data 24 bits (8 bits for each of R, G, and B) long per pixel. Security data 22 is data embedded in the ticket image data 21 in the invisible state and equivalent to Fig. 4. It has data 1 bit long per pixel. Key image data 24 is data as a key for generation of ticket print data and detection (restoration) of security data and it is not opened to a user and has data 1 bit long per pixel.

[0055]

Firstly, at Step 51 of the smoothing process, the program performs the smoothing process on the assumption that the black pixels of the security data 22 are "1" and the white pixels are "0". In this case, the pixels at both ends of the target pixel in the x direction are taken, and an area of 3×1 pixels is separated, and the weights are averaged as shown by Formula (1) below.

[0056]

$$W(i) = (STL(i-1) + 2.STL(i) + STL(i+1))/4 \quad ----- \quad (1)$$

where, W(i): weight average of pixel x=1 and

STL(i): embedded image data = 1 or 0 of pixel x=1

As mentioned above, unless the binary image data is extended to n times at the time of generation of security data, the two-dimensional bar code data of the security data is broken at the time of the smoothing process. It is required to be careful in this regard. As the extension rate n increases, the safety rate that the embedded image data is not broken increases, though data to be hidden is easily exposed.

[0057]

For example, when the key image data 24 is as shown in Fig. 10 and the security data 22 is as shown in Fig. 11, the smoothing results are as shown in Fig. 12. The security data 22 is set at n = 4 and the embedded image data is extended to 4 times. As a margin to embed, two pixels on the outer periphery are set at "0".

[0058]

Next, at Step 52 of phase modulation, the phase of the key image data 24 is modulated on the basis of the results of the smoothing process at Step 51 of the smoothing process and according to the rules of the following formulas (2-1) to (2-3).

[0059]

When W(i)=0: DES(i) = MSK(i) ----- (2-1),
when W(i)=1: DES(i) = MSK(i+2) ----- (2-2), and
in cases other than the above: DES(i) = MSK(i+1) ----- (2-3),
where DES(i): phase modulation result = 1 or 0 of pixel x=i and

MSK(i): key image data = 1 or 0 of pixel x=i.
In this case, the row x=0 and row x=15 are at the end of the image data, so that the smoothing process cannot be performed and hence the phase modulation can neither be performed. Therefore, at the end, the key image data 24 and the security data 22 are exclusively ORed. An example of phase modulation results is shown in Fig. 13.

[0060]

Next, at Step 53 of color difference modulation, the color difference modulation process is performed on the basis of the phase modulation results at Step 52 of phase modulation and according to the rules of the following formulas (3-1) to (3-6). In this case, the three components of R (red), G (green), and B (blue) are calculated separately. An example of color difference modulation results of the red component is shown in Fig. 14.

[0061]

When DES(i)=1: VR(i) = $-\Delta V$ ----- (3-1),

VG(i) = $+\Delta V$ ----------- (3-2),

VB(i) = $+\Delta V$ ----------- (3-3),

when DES(i)=0: VR(i) = $+\Delta V$ --------- (3-4),

VG(i) = $-\Delta V$ ------- (3-5), and

VB(i) = $-\Delta V$ ----------- (3-6),

where VR(i): color difference modulation results of pixel x=1, red component,

integer within the range from -255 to 255,

VG(i): color difference modulation results of pixel x=1, green component,

integer within the range from -255 to 255, and

VB(i): color difference modulation results of pixel x=1, blue component,

integer within the range from -255 to 255.

The color difference amount ΔV is an integer within the range from 0 to 255 which is set beforehand. As the color difference amount ΔV increases, the visualization contrast at the time of restoration of the embedded image data increases and it can be easily reproduced. However, when the visualization contrast increases excessively, the security data is easily exposed. Therefore, it is desirable that the color difference amount ΔV is within the range from 16 to 96, though ΔV = 48 is used here.

[0062]

Finally, at Step 54 of the superimposition process, when the superimposition process indicated by the following formulas (4-1) to (4-3) is performed from the color difference modulation results at Step 53 of color difference modulation and the ticket image data 21, ticket print data 23 is generated.

[0063]

DESR(i) = VR(i) + SRCR(i) ----- (4-1)

DESG(i) = VG(i) + SRCG(i) ----- (4-2)

DESB(i) = VB(i) + SRCB(i) ----- (4-3)

In this case, DESR(i): superimposition results of pixel x=i, red component

integer within the range from 0 to 255,

DESG(i): superimposition results of pixel x=i, green component

integer within the range from 0

to 255,

DESB(i): superimposition results of pixel x=i, blue component

integer within the range from 0 to 255,

SRCR(i): embedded image data of pixel x=i, red component

integer within the range from 0 to 255,

SRCG(i): embedded image data of pixel x=i, green component

integer within the range from 0 to 255, and

SRCB(i): embedded image data of pixel x=i, blue component

integer within the range from 0 to 255.

DESR(i), DESG(i), and DESB(i) are integers within the range from 0 to 255, so that when the calculation result is less than 0, they are set to 0 and when the calculation result is more than 255, they are set to 255.

[0064]

The results of the red component when for all the pixels of the ticket image data 21, (R, G, B) = (127, 127, 127) are shown in Fig. 15. All the values are equal to integers within the range from 0 to 255 and 255 indicates that the amount of red component is most. In Fig. 15, the value of the (0, 0) pixel is 79, and the value of the (1, 0) pixel is 79, and the value of the(2, 0) pixel is 175, and in the portion where no security data is embedded, a pixel having little red component and a pixel having much red component are repeated in units of two pixels.

[0065]

As shown by the formulas (3-1) to (3-3) or the formulas (3-4) to (3-6), the color difference amounts of red, green, and blue are reversed. Therefore, in pixels having much red component, the green and blue colors are less and in pixels having little red component, the other components are much. The red color and the (green, blue)=cyan color have a bearing of a complementary color and when the red color and cyan color are adjacent to each other, they cannot be easily discriminated by the human eyes and are seen as an achromatic color. Red rich pixels and cyan rich pixels are repeatedly arranged in units of several pixels according to the key image data, so that fine color differences of these colors cannot be discriminated by the human eyes and the color difference amount is judged as plus or minus 0.

[0066]

For example, in the aforementioned formula (4-1), it is judged by mistake as:

DESR(i) SRCR(i) ----- (5)

and it is not distinguished that the image data is embedded. Therefore, based on this principle, ticket print data that the security data is embedded in the ticket image data in the invisible state can be created.

[0067]

When printing data by a color printer using the ticket print data, as the color difference amount Δ V increases, it can be discriminated more easily, so that the easiness degree of restoration of the security data increases. However, in this case, the security data embedded in the ticket print data in the invisible state may be easily found out by a third person.

[0068]

Accordingly, when printing and outputting the ticket print data by a color printer, by performing the error diffusion process as an image process and outputting the ticket print data, the security data can be prevented from exposure without breaking the security data. By doing this, the density of each pixel of the ticket print data is compensated by the error diffusion process and the data of the security data in the invisible state is saved on a macro basis.

[0069]

When the error diffusion process is performed, the low frequency component decreases and the high frequency component increases. The security data embedded in the ticket print data is composed of a high frequency component, so that other high frequency components are mixed in by the error diffusion process and hence the security data enters the state that those other components cannot be visually discriminated.

[0070]

Next, the ticket display data generation method will be explained.

[0071]

Ticket display data that the ticket print data is partially reduced, and the ticket image data and security data embedded in the invisible state are partially broken, and they cannot be used as they are is generated. Firstly, the ticket print data shown in Fig. 15 is separated into areas of 3×3 pixels and the smoothing process is performed for them. The process simply gets the average and the results are shown in Fig. 16. When the pixel data at the vertex of the area of 4×4 pixels is left from the smoothing results shown in Fig. 16 and the remainder is erased (thinned out), the results are as shown in Fig. 17. This is ticket display data.

[0072]

In this case, the data amount is about 1/4 of the ticket print data. The print image resolution is generally about 300 to 600 dpi, while the image resolution of the display screen is about 100 dpi and hence the data amount is about 1/3 to 1/6. Therefore, there is no problem.

[0073]

As mentioned above, when the ticket print data is not displayed on the user terminal device 11 as it is and ticket display data is generated by reducing the ticket print data and breaking the security data and displayed on the user terminal device 11, since the process (display) is fast because the data amount is small and the security data and ticket image data are partially broken, even if it is attempted to unfairly get them by hard copy of the screen, they cannot be used. Therefore, there is an advantage that the security improves more.

[0074]

Since the ticket print data and ticket display data are not apparently different from general images, for example, the general-purpose image formats such as JPEG and TIFF can be used and since they can be processed by the application for handling general images, the system can be constructed comparatively easily.

[0075]

Even if the image format of the ticket print data is converted to another one in the system, the embedded security data remains as it is and no problem arises.

[0076]

Meanwhile, the ticket 14 that the ticket print data is printed and output by the ticket printer 13 such as a color printer is used by a user at the concert place. In this case, the system side detects the security data of the used ticket 14 and hence can discriminate the truth of the ticket. It will be explained hereunder in detail.

[0077]

The image on the ticket surface of the ticket 14 which is printed on a paper by the ticket printer 13 is read by an optical reading means such as a scanner, converted to digital data, and put into the state shown in Fig. 15 and the security data 22 is restored.

[0078]

To restore the security data 22, the key image data 24 shown in Fig. 10 is used. The key image data 24 and the value of the ticket surface image of the ticket print data 23 read by the scanner are allowed to have a one-to-one correspondence and it is judged that in the portion where the value of the key image data 24 is 1, the data of the ticket print data 23 is valid and in the portion where the value of the key image data 24 is 0, the data of the ticket print data 23 is invalid. The results are shown in Fig. 18. In the drawing, the hatched pixels are invalid data. The valid data (represented by a void) in Fig. 18 are separated in the predetermined size.

[0079]

Since the security data 22 of this embodiment is set at n = 4 and the security data 22 is extended to 4 times, the two pixels of the margin to embed on the periphery are removed and then the security data 22 is separated in units of 4×4 pixels. When the value of valid data within the range of 4×4 pixels is a red rich value (175 in this embodiment), the embedded image data (security data) is 1 and when it is a cyan rich value (79 in this embodiment), the embedded image data is 0. When the valid data includes both red rich value and cyan rich value, the larger value is used.

[0080]

The cause is the smoothing process of the synthetic process. The results when the embedded image data (security data) 22 is restored by this method is shown in Fig. 19. The portions of the thick line frames shown in the drawing are portions of the security data 22 and coincide with those shown in Fig. 11 and it shows that the security data 22 is completely restored.

[0081]

In this embodiment, for example, data is printed by a sublimation type thermal printer at a resolution of 400 dpi and read by an optical scanner at a resolution of 1200 dpi and then the restoration process is performed. The security data 22 can be restored without trouble.

[0082]

By the second restoration and detection method for the security data, when a reproduced sheet having the transmission distribution rate of the same pattern as that of the key image data 24 is physically superimposed on the print surface of the ticket 14, the security data 22 can be seen visually and the logo mark in the security data 22 can be directly confirmed by the check by the human sense of sight. This method does not require troublesome operations and a complicated device, so that there is an advantage that the truth can be simply discriminated at any location.

[0083]

Furthermore, as a third security data

restoration and detection method, a method for thinning out a value read by an optical means will be explained hereunder. The red component of a value read by a scanner is assumed as shown in Fig. 15. In this embodiment, a check pattern in units of 4×2 is used for the synthetic process, so that it is thinned out in units of 4 pixels. To this value, the extension rate n at the time of generation of the security data is also related and the relation of "lattice unit of check pattern x extension rate n ≧ No. of pixels to be thinned out" is held.

[0084]

When the pixel data shown in Fig. 15 is thinned out in units of 4 pixels, the results shown in Fig. 20 are obtained. In this state, the pixel data is insufficient, so that when the areas of 4×2 with the remaining pixels set at vertexes are all set to the same value, the results shown in Fig. 21 are obtained and they are shifted by 2 pixels respectively in the x direction and y direction, though it shows that the security data 22 shown in Fig. 11 is restored 100%. By thinning out the read image data like this, the number of pixels for which the process for restoration is to be performed reduces, so that the security data 22 can be restored at high speed.

[0085]

By detecting the existence of the security data 22 embedded in the used ticket 14 as mentioned above, the truth of the ticket 14 can be simply discriminated. For example, even when the ticket 14 is passed into third person's hands and unfairly copied by a color copying machine, since the inquiry serial number is put in the security data 22, the history of the ticket such as when, where, and to whom the ticket is issued can be simply found and the unfair route can be simply ascertained.

[0086]

In this embodiment, the synthetic process is performed using a check pattern in units of 4×2 as a key. Therefore, when the synthetic process is performed using a check pattern of 1×1, the effect of copy prevention for a color copying machine is obtained more. The reason is that when a square lattice of 1×1 or 2×2 is used, in the ticket print data, red rich and cyan rich pixel data are arranged alternately and regularly by the synthetic process.

[0087]

The sensor in the scanner portion such as a color copying machine is not a point but has a finite area, so that for example, even if the reading resolution of the scanner is the same as the ticket print resolution, the sensor pixels of the scanner and the pixels of the ticket print data are seen in the finely shifted state. In this case, the red and cyan colors have a relation of complementary color, so that it is difficult to separate pixels arranged at a very fine pitch, and they are recognized as a gray color by mistake not only by human eyes but also by the sensor, and the copying operation cannot be performed normally.

[0088]

According to this embodiment, it is possible to remarkably enhance the security of tickets. However, since the security data is embedded in the invisible state, some means is necessary to restore it and it is troublesome to perform the operation for all tickets.

[0089]

Therefore, it is necessary to distinguish a ticket with the security data embedded in the invisible state from a ticket with no security data embedded which is guaranteed to be a regular ticket by some means. For example, when a means for printing the logo mark of a ticket with the security data embedded in red and printing the logo mark of a ticket with no security data embedded in blue is used, tickets can be simply checked and the time and cost can be saved greatly.

[0090]

Fig. 22 schematically shows the situation from issuing of a ticket to detection of the security data which is mentioned above. For the ticket image data 21, a landscape picture is used. For the security data 22, the logo mark "JAPAN" as copyright data and the two-dimensional bar code for checking by the human sense of sight and checking by the machine which are converted to security data according to the procedure indicated in this embodiment are used.

[0091]

Firstly, the synthetic process is performed for the ticket image data 21, the security data 22, and the key image data 24 by the aforementioned method and the ticket print data 23 is generated. The image of the ticket print data 23 is seen just as a landscape picture by human eyes, though the copyright data and others are embedded in it in the invisible state. From the ticket print data 23, the ticket display data 25 is generated by the method indicated in this embodiment.

[0092]

Next, the ticket print data 23 and the ticket display data 25 which are generated are sent to a user requesting ticket issue via the network. The user receiving the ticket display data 25 displays the ticket display data 25 on the display of the user terminal device 11, confirms the contents, and then prints and outputs the ticket print data 23 by the ticket printer 13 such as a color printer and obtains the ticket 14.

[0093]

The user can use the ticket 14 issued and the system side detects the security data of the used ticket 14 using the key image data and discriminates the truth by checking the data base and security data.

[0094]

In the ticket 14 issued, the security data including the copyright data is embedded in the invisible state, so that by the aforementioned restoration method, the copyright data can be restored.

[0095]

Fig. 23 shows an example that the ticket issue method of the present invention is applied to an electronic stamp. Fig. 23(a) shows ticket print data, and Fig. 3(b) shows a stamp image portion, and Fig. 23(c) shows security data embedded in the stamp image portion in the invisible state. Particularly, to allow a user to issue an article equivalent to money in value like a stamp, the security is important. When the security data is also embedded in an electronic stamp in the invisible state like the aforementioned concert ticket and the ticket (stamp) print data is directly printed on an envelope, an electronic stamp can be realized.

[0096]

In the case of such a mail, the mechanical process such as reading of the address is generally performed, so that by discriminating the truth by reading the security data embedded in the electronic stamp by the sensor at that time, the security can be maintained. By printing the destination address and name at the same time when printing and outputting a stamp by a color printer like this, the cost can be reduced greatly.

[0097]

[Effects of the Invention]

As mentioned above in detail, according to the present invention, a ticket issue method which can simply issue tickets with high security via a communication means such as a network or telephone lines can be provided.

[0098]

Furthermore, according to the present invention, a ticket check method which can simply discriminate the truth of tickets issued by the aforementioned ticket issue method and when an unfair ticket is found, can easily conduct a follow-up study of it can be provided.

[Brief Description of the Drawings]

Fig. 1 is a block diagram schematically showing the constitution of a ticket issue system for realizing the ticket issue method relating to the embodiment of the present invention.

Fig. 2 is a flow chart for explaining the operation procedure of ticket issue.

Fig. 3 is a drawing showing an example of ticket image data when the present invention is applied to concert tickets.

Fig. 4 is a drawing showing an example of security data when the present invention is applied to concert tickets.

Fig. 5 is a drawing showing an example of ticket print data when the present invention is applied to concert tickets.

Fig. 6 is a drawing for explaining converting to a binary image by a two-dimensional code of security data.

Fig. 7 is a drawing for explaining converting to a binary image by a two-dimensional code of security data.

Fig. 8 is a drawing for explaining converting to a binary image by a two-dimensional code of security

data.

Fig. 9 is a drawing for explaining the preparation procedure of ticket print data.

Fig. 10 is a drawing showing a concrete calculation example in preparation of ticket print data.

Fig. 11 is a drawing showing a concrete calculation example in preparation of ticket print data.

Fig. 12 is a drawing showing a concrete calculation example in preparation of ticket print data.

Fig. 13 is a drawing showing a concrete calculation example in preparation of ticket print data.

Fig. 14 is a drawing showing a concrete calculation example in preparation of ticket print data.

Fig. 15 is a drawing showing a concrete calculation example in preparation of ticket print data.

Fig. 16 is a drawing showing a concrete calculation example in preparation of ticket print data.

Fig. 17 is a drawing showing a concrete calculation example in preparation of ticket print

data.

Fig. 18 is a drawing showing a concrete calculation example in preparation of ticket print data.

Fig. 19 is a drawing showing a concrete calculation example in preparation of ticket print data.

Fig. 20 is a drawing for explaining the thinning-out process in the third reproduction method.

Fig. 21 is a drawing for explaining the interpolation process in the third reproduction method.

Fig. 22 is a drawing schematically showing the ticket issue method.

Fig. 23 is a drawing for explaining an example that the ticket issue method of the present invention is applied to an electronic stamp.

[Description of Numerals]

A: Apparatus on the user side, B: Apparatus on the system side, C: Network, 11: User terminal device, 13: Ticket printer, 14: Ticket, 16: Host computer/server, 18: Data base, 19: Security data detecting system, 21: Ticket image data, 22: Security data, 23: Ticket print data, 24: Key image data, 51: Smoothing step, 52: Phase modulation step, 53: Color difference modulation step, 54: Superimposition step

[Document Name] Abstract

[Abstract]

[Problem] The present invention provides a ticket issue method which can simply issue tickets with high security via a communication means such as a network or telephone lines.

[Solving Means] The ticket issue method generates security data from ticket issue request data sent from a user via a network and user identification data, also generates ticket image data from the ticket issue request data, embeds the generated security data in the generated ticket image data in the invisible state, thus generates ticket print data, and sends the generated ticket print data to the user via the network and the user prints a ticket on the basis of the sent ticket print data.

[Selected Drawing] Fig. 2

[Document Name] Drawing

[Fig. 1]

1 User side

11 User terminal device

12 Dedicated client software

13 Ticket printer (Color printer)

2 Print

14 Ticket

3 Use

15 Concert, etc.

4 Inspection

5 System side

18 Data base

- Ticket data
- User data
- Terminal data

6 Check

16 Host computer/server

17 Dedicated server software

7 Check

19 Security data detecting system

[Fig. 2]

1 User side

2 Start

S1 Start the user terminal and dedicated client software.

S2 Request input and connection of user identification data.

S5 Connect to the host computer.

S7 Display the service menu.

S8 Select the desired service and input the ticket issue request data.

S15 Display the ticket display data on the display.

S16 Print the ticket print data by the ticket printer.

S17 Use the ticket.

3 End

4 System side

5 Start

S3 Check with the data base.

S4 The connection to the host computer is permitted.

S6 Send the service menu.

S9 Check with the data base.

S10 Prepare security data from the user identification data and ticket issue request data.

S11 Prepare ticket image data from the ticket issue request data.

S12 Prepare ticket print data from the security data and ticket image data.

S13 Prepare ticket display data from the ticket print data.

S14 Send the ticket print data and ticket display

data.

S18 Check the used ticket by the security data detecting system.

6 End

[FIG. 3]

31 '98 △△△△ WORLD CHAMPIONSHIP SERIES THE□□ MATCH

JAPAN ○○○○ RACE

<< FINAL MATCH ADMISSION TICKET >>

INQUIRY: TO ◇◇◇◇◇◇◇◇

CIRCUIT

32 1998, 12.24

33 RESERVED SEAT: 12

34 FINAL MATCH ADMISSION TICKET: ADULT: ¥10000

35 19989925123412345678

36 TICKET EAST-WEST-SOUTH-NORTH

[Fig. 8]

1 In the case of n=2

[Fig. 9]

21 Ticket image data

22 Security data

24 Key image data

1 Synthetic process

51 Smoothing

52 Phase modulation

53 Color difference modulation

2 Color difference ΔV

54 Superimposition

23 Ticket print data

[Fig. 10] Key image

[Fig. 11] Security data

[Fig. 12] Smoothing result

[Fig. 13] Phase modulation result

[Fig. 14] Color difference modulation result

Red component

[Fig. 15] Superimposition result Red component

[Fig. 16] Prepare ticket display data

Smoothing Red component

[Fig. 17] Prepare ticket display

Thinned out process Red component

[Fig. 18] Restoration result (a) Red component

[Fig. 19] Restoration result (b) Red component

[Fig. 20] Thinned out process result

[Fig. 21] Interpolation process result

[Fig. 22]

1 Embedded invisibly in composite image

2 Combining process

3 Changed into visible state

4 Ticket display data

5 Making

6 Ticket print data

7 Transmitting

8 System side

9 Superimpose on key image data

10 User side

11 Displayed on display device

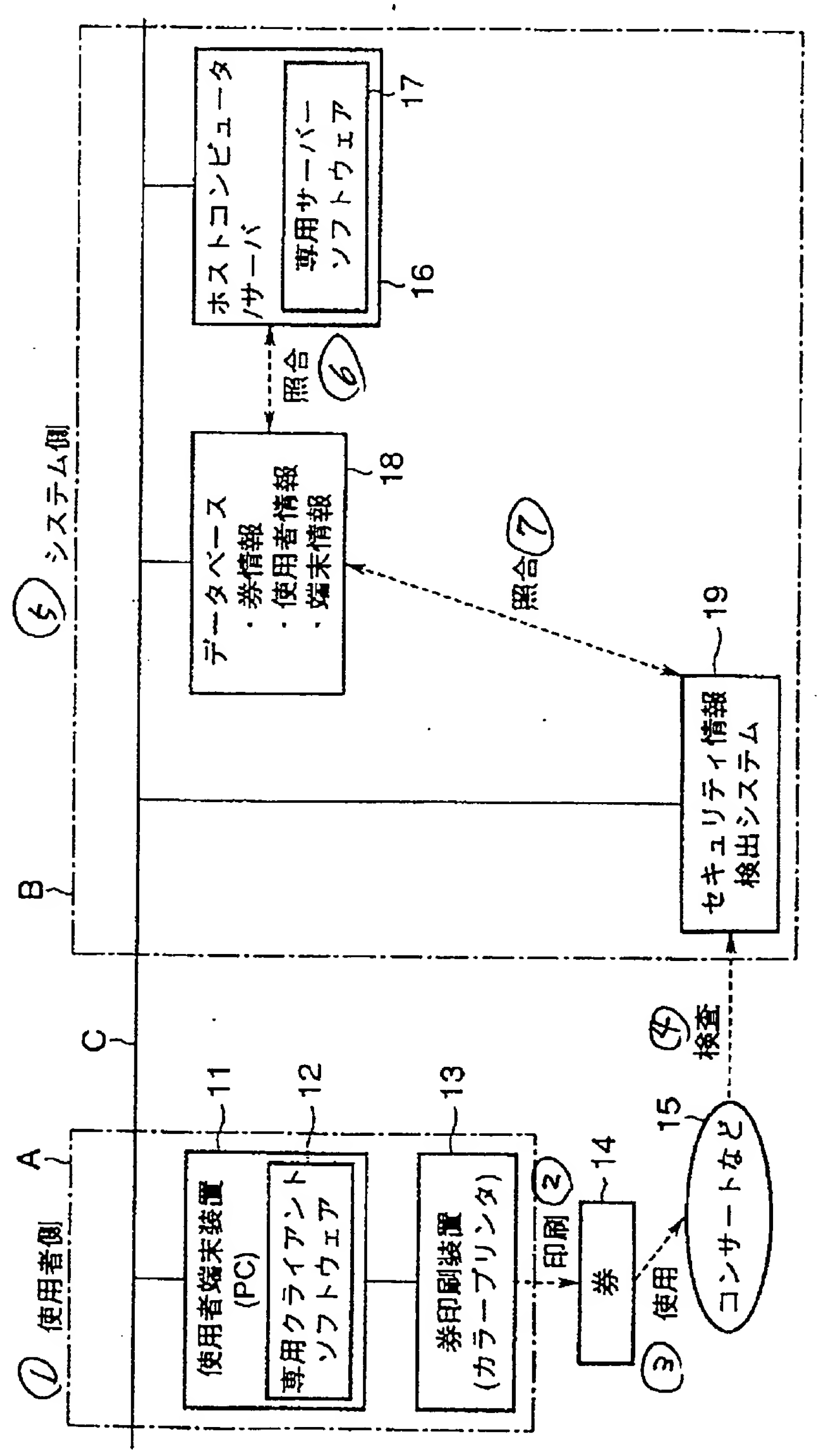
12 Print by color printer

13 A ticket

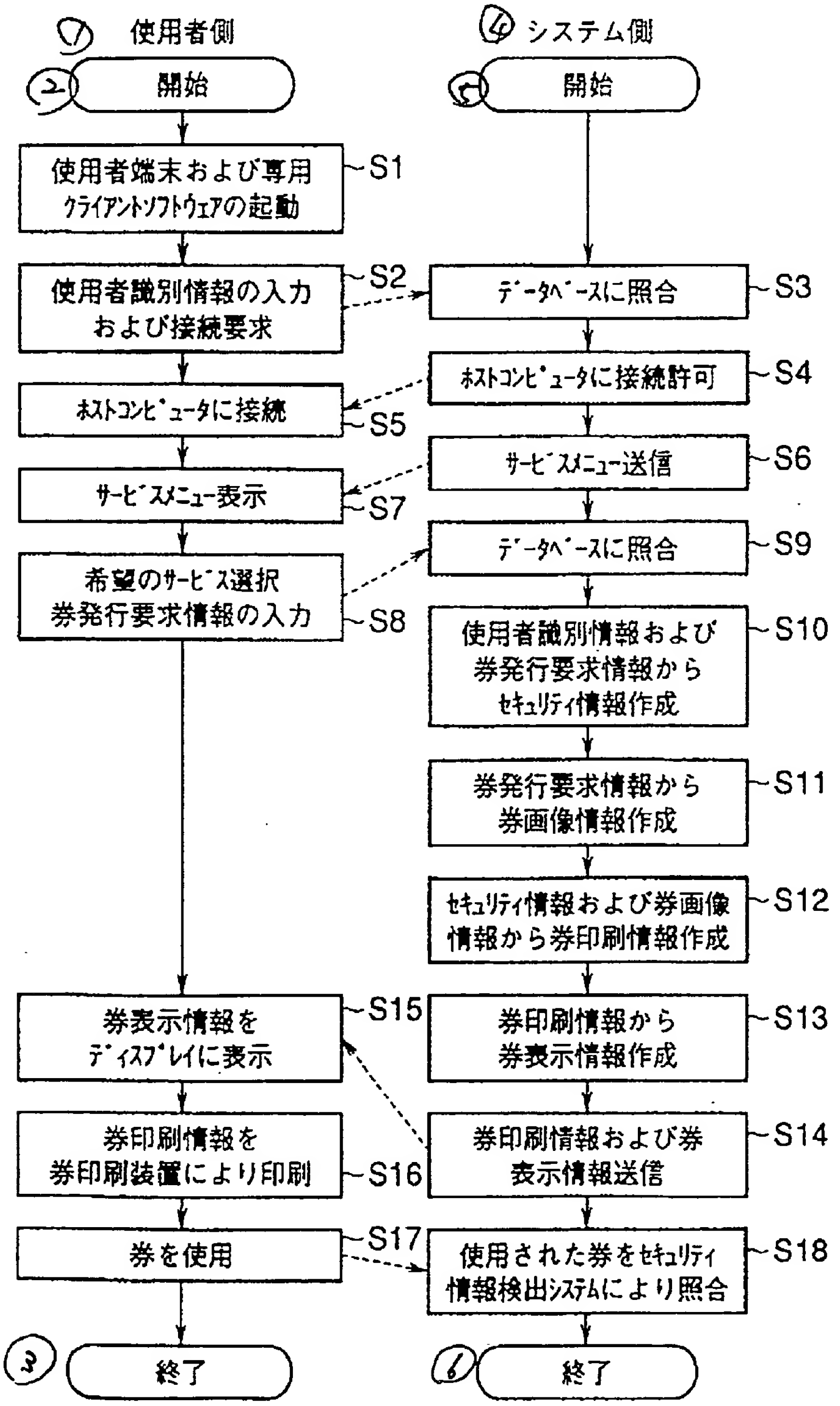
14 Use

【書類名】　図面

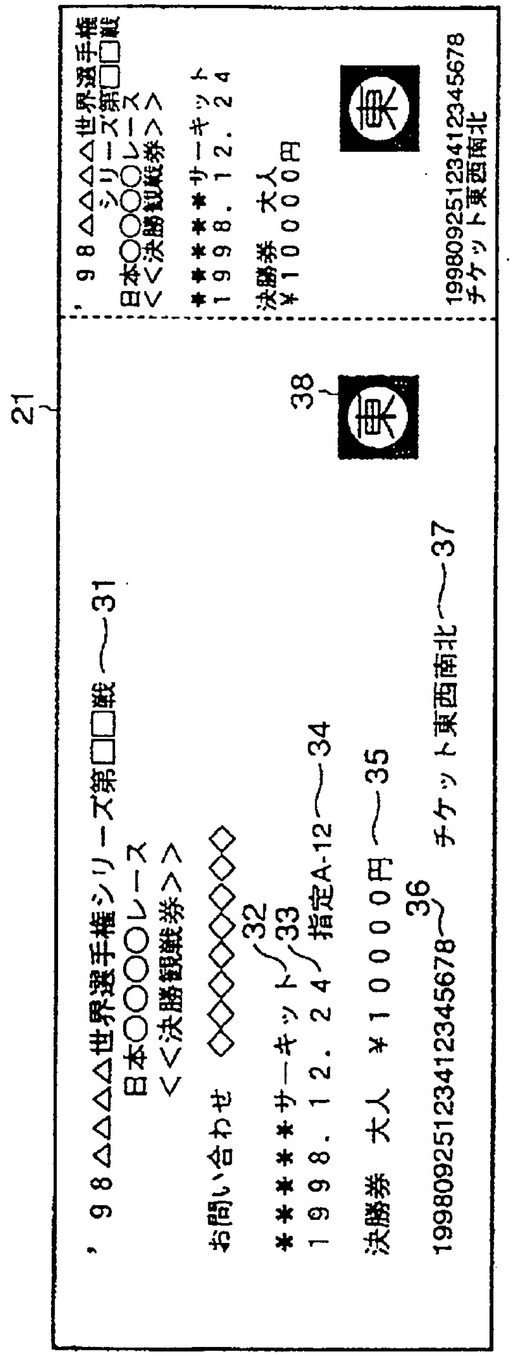
【図1】


①
使用者側
A
11
使用者端末装置
(PC)
12
専用クライアント
ソフトウェア
13
券印刷装置
(カラープリンタ)
印刷
②
14
券
③
使用
15
コンサートなど
④
検査
C
B
⑤
システム側
ホストコンピュータ
／サーバ
16
専用サーバー
ソフトウェア
17
照合
⑥
データベース
・券情報
・使用者情報
・端末情報
18
照合
⑦
19
セキュリティ情報
検出システム

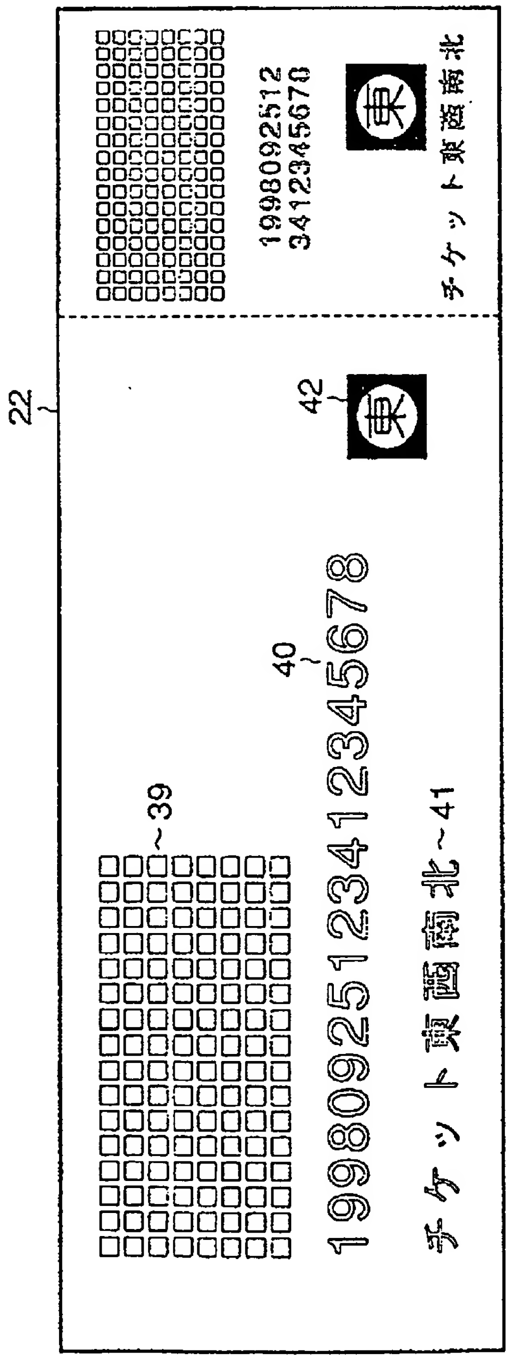
【図２】


1
使用者側
4
システム側
2
開始
5
開始
使用者端末および専用クライアントソフトウェアの起動
S1
使用者識別情報の入力および接続要求
S2
データベースに照合
S3
ホストコンピュータに接続許可
S4
ホストコンピュータに接続
S5
サービスメニュー送信
S6
サービスメニュー表示
S7
データベースに照合
S9
希望のサービス選択
券発行要求情報の入力
S8
使用者識別情報および券発行要求情報からセキュリティ情報作成
S10
券発行要求情報から券画像情報作成
S11
セキュリティ情報および券画像情報から券印刷情報作成
S12
券表示情報をディスプレイに表示
S15
券印刷情報から券表示情報作成
S13
券印刷情報を券印刷装置により印刷
S16
券印刷情報および券表示情報送信
S14
券を使用
S17
使用された券をセキュリティ情報検出システムにより照合
S18
3
終了
6
終了

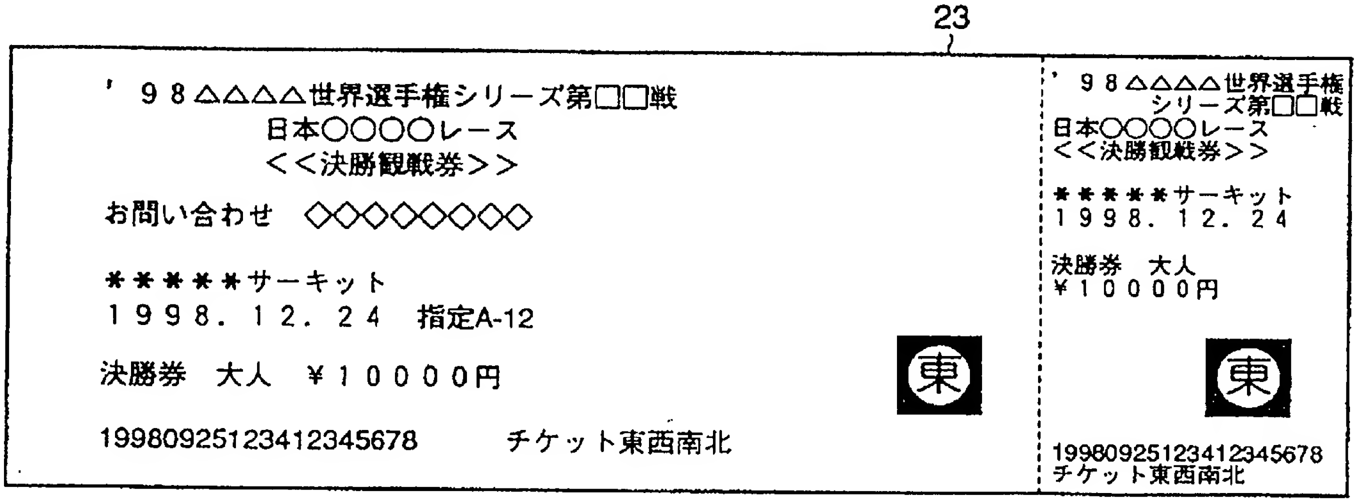
【図３】


21
'９８△△△△世界選手権シリーズ第□□戦
31
日本○○○レース
<<決勝観戦券>>
お問い合わせ　◇◇◇◇◇◇◇◇
＊＊＊＊＊サーキット
32
１９９８．１２．２４
33
指定A-12
34
決勝券　大人　¥１０００円
35
19980925123412345678
36
チケット東西南北
37
東
38
'９８△△△△世界選手権
シリーズ第□□戦
日本○○○レース
<<決勝観戦券>>
＊＊＊＊＊サーキット
１９９８．１２．２４
決勝券　大人
¥１０００円
19980925123412345678
チケット東西南北
東

【図４】


22
42
40
39
41
東
1998092512
3412345678
19980925123412345678
チケット東西南北

【図5】



’９８△△△△世界選手権シリーズ第□□戦
日本○○○○レース
＜＜決勝観戦券＞＞

お問い合わせ　◇◇◇◇◇◇◇◇

＊＊＊＊＊サーキット
１９９８．１２．２４　指定A-12

決勝券　大人　￥１００００円

19980925123412345678　チケット東西南北

東

’９８△△△△世界選手権
シリーズ第□□戦
日本○○○○レース
＜＜決勝観戦券＞＞

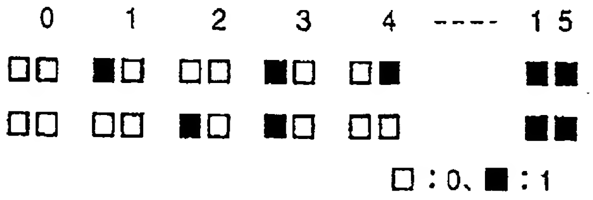
＊＊＊＊＊サーキット
１９９８．１２．２４

決勝券　大人
￥１００００円

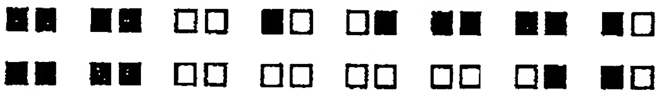
東

19980925123412345678
チケット東西南北

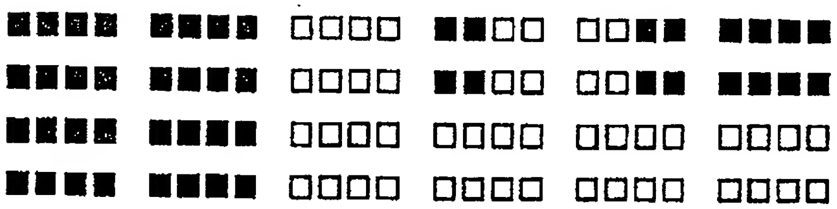
【図6】



【図7】

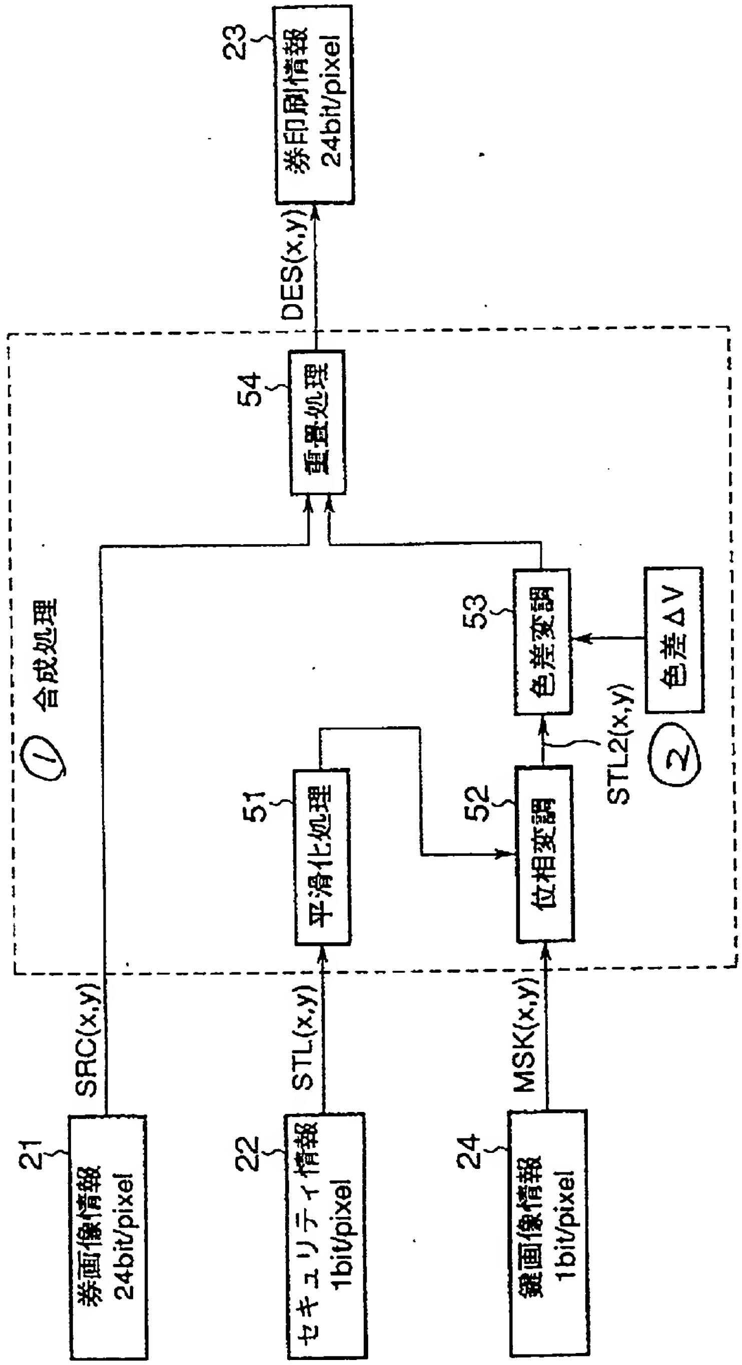


【図8】



① n=2の場合

【図９】


23
券印刷情報
24bit/pixel
DES(x,y)
54
重畳処理
①
合成処理
53
色差変調
色差ΔV
STL2(x,y)
②
51
平滑化処理
52
位相変調
SRC(x,y)
STL(x,y)
MSK(x,y)
21
券画像情報
24bit/pixel
22
セキュリティ情報
1bit/pixel
24
鍵画像情報
1bit/pixel

【図１０】

鍵画像

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
2	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
3	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
4	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
5	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
6	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
7	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
8	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
9	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
10	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
11	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1

【図１１】

セキュリティ情報

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0
3	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0
4	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0
5	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0
6	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0
7	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0
8	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0
9	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

【図12】

平滑化処理結果

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	x	0	0	0	0	0	0	0	0	0	0	0	0	0	0	x
1	x	0	0	0	0	0	0	0	0	0	0	0	0	0	0	x
2	x	0.25	0.75	1	1	0.75	0.25	0	0	0.25	0.75	1	1	0.75	0.25	x
3	x	0.25	0.75	1	1	0.75	0.25	0	0	0.25	0.75	1	1	0.75	0.25	x
4	x	0.25	0.75	1	1	0.75	0.25	0	0	0.25	0.75	1	1	0.75	0.25	x
5	x	0.25	0.75	1	1	0.75	0.25	0	0	0.25	0.75	1	1	0.75	0.25	x
6	x	0	0	0	0	0.25	0.75	1	1	1	1	1	1	0.75	0.25	x
7	x	0	0	0	0	0.25	0.75	1	1	1	1	1	1	0.75	0.25	x
8	x	0	0	0	0	0.25	0.75	1	1	1	1	1	1	0.75	0.25	x
9	x	0	0	0	0	0.25	0.75	1	1	1	1	1	1	0.75	0.25	x
10	x	0	0	0	0	0	0	0	0	0	0	0	0	0	0	x
11	x	0	0	0	0	0	0	0	0	0	0	0	0	0	0	x

【図１３】

位相変調結果

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
2	1	1	0	1	0	0	0	0	1	1	0	1	0	0	0	0
3	0	0	1	0	1	1	1	1	0	0	1	0	1	1	1	1
4	1	1	0	1	0	0	0	0	1	1	0	1	0	0	0	0
5	0	0	1	0	1	1	1	1	0	1	1	0	1	1	1	1
6	1	1	0	0	1	1	0	1	0	0	1	1	0	0	0	0
7	0	0	1	1	0	0	1	0	1	1	0	0	1	1	1	1
8	1	1	0	0	1	1	0	1	0	0	1	1	0	0	0	0
9	0	0	1	1	0	0	1	0	1	1	0	0	1	1	1	1
10	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
11	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1

【図14】

色差変調結果　赤成分

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	-48	-48	+48	+48	-48	-48	+48	+48	-48	-48	+48	+48	-48	-48	+48	+48
1	+48	+48	-48	-48	+48	+48	-48	-48	+48	+48	-48	-48	+48	+48	-48	-48
2	-48	-48	+48	-48	+48	+48	+48	+48	-48	+48	+48	-48	+48	+48	+48	+48
3	+48	+48	-48	+48	-48	-48	-48	-48	+48	-48	-48	+48	-48	-48	-48	-48
4	-48	-48	+48	-48	+48	+48	+48	+48	-48	+48	+48	-48	+48	+48	+48	+48
5	+48	+48	-48	+48	-48	-48	-48	-48	+48	-48	-48	+48	-48	-48	-48	-48
6	-48	-48	+48	+48	-48	+48	+48	-48	+48	+48	-48	-48	+48	+48	+48	+48
7	+48	+48	-48	-48	+48	-48	-48	+48	-48	-48	+48	+48	-48	-48	-48	-48
8	-48	-48	+48	+48	-48	+48	+48	-48	+48	+48	-48	-48	+48	+48	+48	+48
9	+48	+48	-48	-48	+48	-48	-48	+48	-48	-48	+48	+48	-48	-48	-48	-48
10	-48	-48	+48	+48	-48	-48	+48	+48	-48	-48	+48	+48	-48	-48	+48	+48
11	+48	+48	-48	-48	+48	-48	-48	-48	+48	+48	-48	-48	-48	+48	-48	-48

【図１５】

重畳処理結果　赤成分

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	79	79	175	175	79	79	175	175	79	79	175	175	79	79	175	175
1	175	175	79	79	175	175	79	79	175	175	79	79	175	175	79	79
2	79	175	175	79	175	175	175	175	79	175	175	79	175	175	175	175
3	175	79	79	175	79	79	79	79	175	79	79	175	79	79	79	79
4	79	175	175	79	175	175	175	175	79	175	175	79	175	175	175	175
5	175	79	79	175	79	79	79	79	175	79	79	175	79	79	79	79
6	79	79	175	175	79	175	175	79	175	175	79	79	175	175	175	175
7	175	175	79	79	175	79	79	175	79	79	175	175	79	79	79	79
8	79	79	175	175	79	175	175	79	175	175	79	79	175	175	175	175
9	175	175	79	79	175	79	79	175	79	79	175	175	79	79	79	79
10	79	79	175	175	79	79	175	175	79	79	175	175	79	79	175	175
11	175	175	79	79	175	175	79	79	175	175	79	79	175	175	79	79

【図１６】

券表示情報作成ー平滑化処理　赤成分

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
1	×	132	132	132	132	143	143	132	132	132	132	132	132	143	143	×
2	×	132	122	122	132	132	122	122	132	132	122	122	132	132	122	×
3	×	132	132	132	132	143	143	132	132	132	132	132	132	143	143	×
4	×	122	122	122	122	111	111	122	122	122	122	122	122	111	111	×
5	×	122	132	132	132	132	132	132	132	132	122	122	132	143	143	×
6	×	122	122	122	122	111	111	122	122	122	122	122	122	111	111	×
7	×	122	132	132	132	132	132	132	132	132	122	122	132	143	143	×
8	×	132	122	122	122	122	122	122	122	122	132	132	122	111	111	×
9	×	122	132	132	122	122	132	132	122	122	132	132	122	122	132	×
10	×	132	122	122	122	122	122	122	122	122	132	132	122	111	111	×
11	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×

【図１７】

券表示情報作成ー間引き処理　赤成分

	0	1	2	3
0	132	143	132	143
1	122	132	132	143
2	122	122	122	122

【図18】

復元結果(a)　赤成分

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	79	79	175	175	79	79	175	175	79	79	175	175	79	79	175	175
1	175	175	79	79	175	175	79	79	175	175	79	79	175	175	79	79
2	79	175	175	79	175	175	175	175	79	175	175	79	175	175	175	175
3	175	79	79	175	79	79	79	79	175	79	79	175	79	79	79	79
4	79	175	175	79	175	175	175	175	79	175	175	79	175	175	175	175
5	175	79	79	175	79	79	79	79	175	79	79	175	79	79	79	79
6	79	79	175	175	79	175	175	79	175	175	79	79	175	175	175	175
7	175	175	79	79	175	79	79	175	79	79	175	175	79	79	79	79
8	79	79	175	175	79	175	175	79	175	175	79	79	175	175	175	175
9	175	175	79	79	175	79	79	175	79	79	175	175	79	79	79	79
10	79	79	175	175	79	79	175	175	79	79	175	175	79	79	175	175
11	175	175	79	79	175	175	79	79	175	175	79	79	175	175	79	79

【図１９】

復元結果(b)　赤成分

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
2	X	X	1	1	1	1	0	0	0	0	1	1	1	1	X	X
3	X	X	1	1	1	1	0	0	0	0	1	1	1	1	X	X
4	X	X	1	1	1	1	0	0	0	0	1	1	1	1	X	X
5	X	X	1	1	1	1	0	0	0	0	1	1	1	1	X	X
6	X	X	0	0	0	0	1	1	1	1	1	1	1	1	X	X
7	X	X	0	0	0	0	1	1	1	1	1	1	1	1	X	X
8	X	X	0	0	0	0	1	1	1	1	1	1	1	1	X	X
9	X	X	0	0	0	0	1	1	1	1	1	1	1	1	X	X
10	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
11	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

【図２０】

間引き処理結果　赤成分

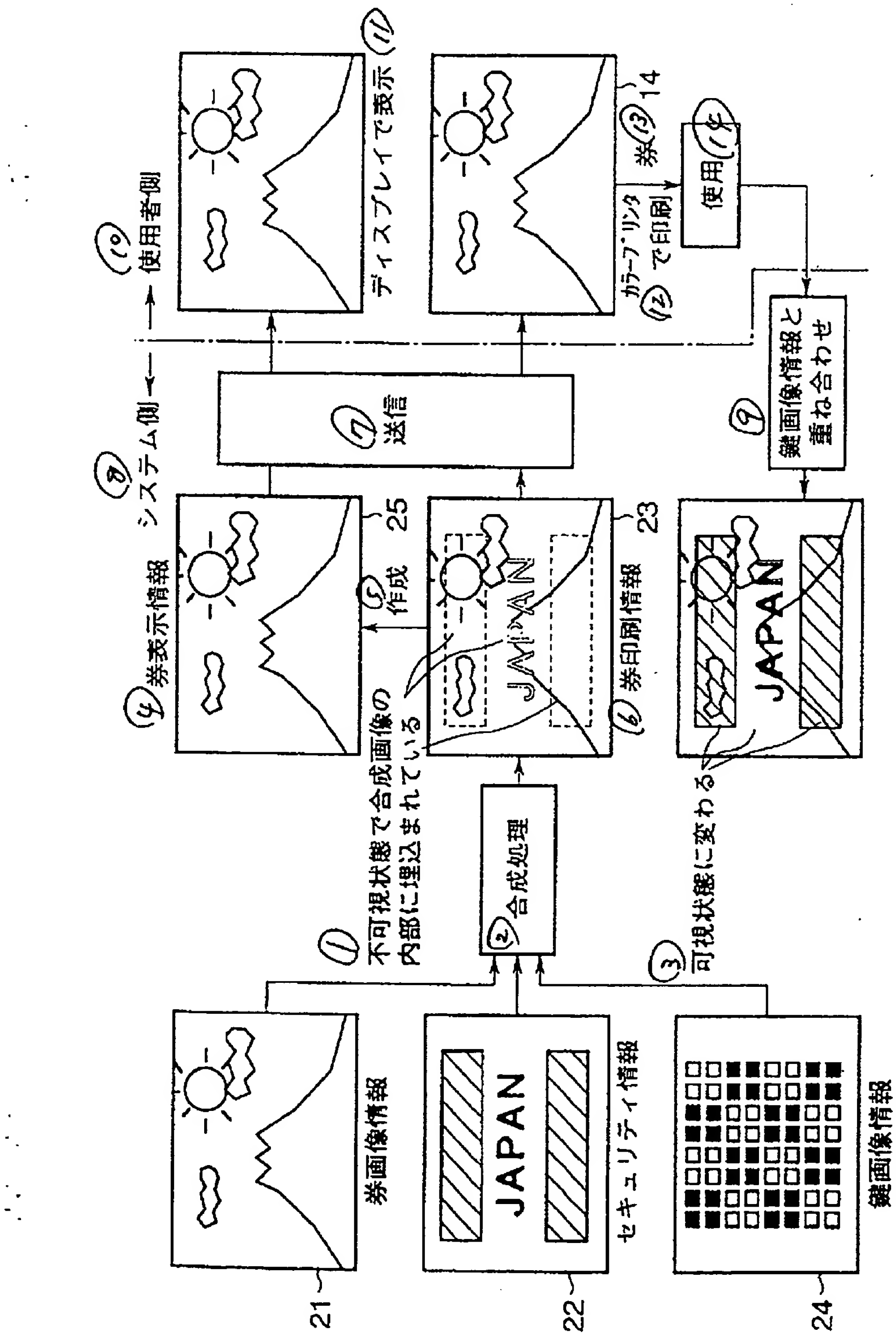
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	79				79				79				79			
1																
2																
3																
4	79				175				79				175			
5																
6																
7																
8	79				79				175				175			
9																
10																
11																

【図２１】

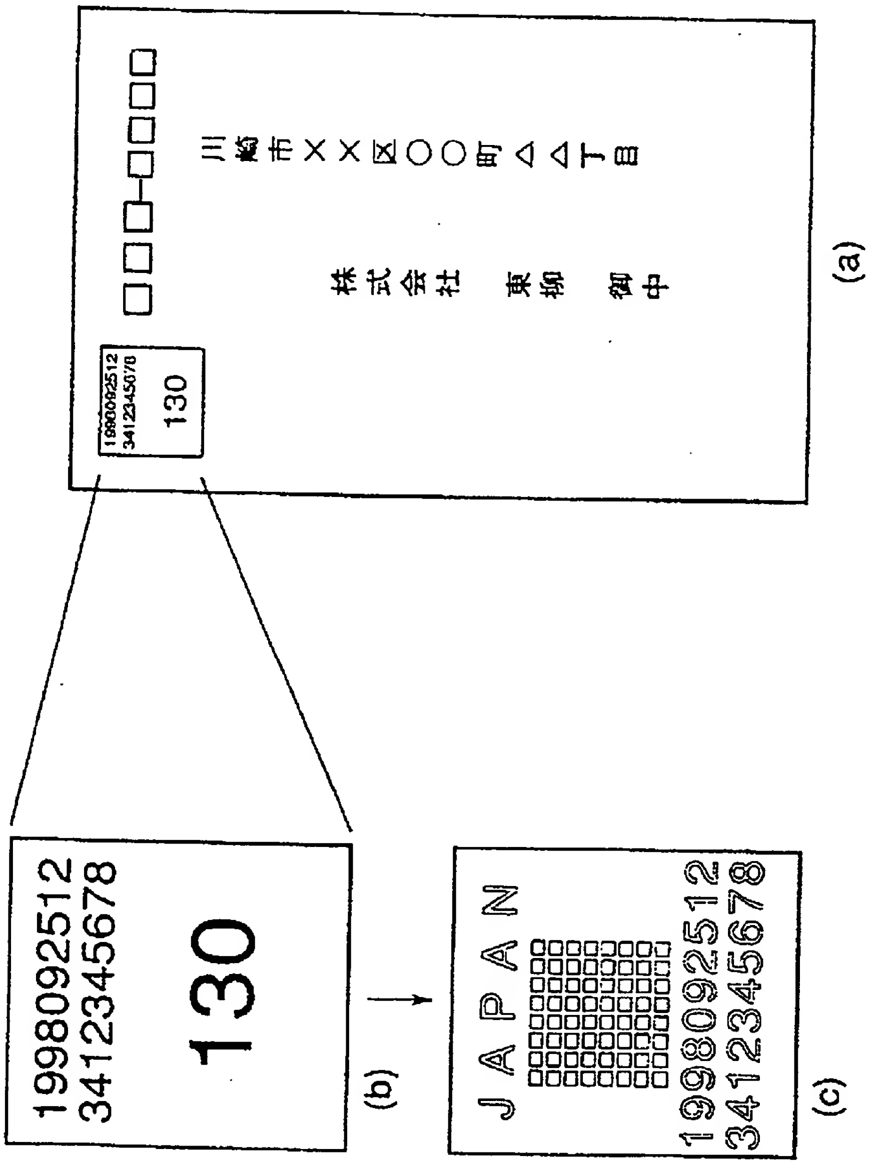
補完処理結果　赤成分

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	79	79	79	79	79	79	79	79	79	79	79	79	79	79	79	79
1	79	79	79	79	79	79	79	79	79	79	79	79	79	79	79	79
2	79	79	79	79	79	79	79	79	79	79	79	79	79	79	79	79
3	79	79	79	79	79	79	79	79	79	79	79	79	79	79	79	79
4	79	79	79	79	175	175	175	175	79	79	79	79	175	175	175	175
5	79	79	79	79	175	175	175	175	79	79	79	79	175	175	175	175
6	79	79	79	79	175	175	175	175	79	79	79	79	175	175	175	175
7	79	79	79	79	175	175	175	175	79	79	79	79	175	175	175	175
8	79	79	79	79	79	79	79	79	175	175	175	175	175	175	175	175
9	79	79	79	79	79	79	79	79	175	175	175	175	175	175	175	175
10	79	79	79	79	79	79	79	79	175	175	175	175	175	175	175	175
11	79	79	79	79	79	79	79	79	175	175	175	175	175	175	175	175

【図22】


⑩ 使用者側
システム側 ⑧
⑪ ディスプレイで表示
④ 券表示情報
25
⑤ 作成
⑥ 券印刷情報
23
⑦ 送信
⑫ カラープリンタで印刷
券 ⑬
14
使用 ⑭
⑨ 鍵画像情報と重ね合わせ
① 不可視状態で合成画像の内部に埋込まれている
② 合成処理
③ 可視状態に変わる
JAPAN
券画像情報
セキュリティ情報
鍵画像情報
21
22
24

【図23】


□□□-□□□□
川崎市××区○○町△△丁目
株式会社　東芝　御中
1998092512
3412345678
130
(a)
1998092512
3412345678
130
(b)
JAPAN
1998092512
3412345678
(c)